UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 4:04CR624 RWS
	)	
JOHN LARKIN TROTTER,	)	
	)	
Defendants.	)	

MEMORANDUM AND RECOMMENDATION
OF UNITED STATES MAGISTRATE JUDGE

The above matter was referred to the undersigned United States Magistrate Judge pursuant to 28 U.S.C. §636(b). At the status conference on June 22, 2005, the Defendant indicated that he would be withdrawing his previously filed motion to suppress evidence and statements, and requesting leave to file a motion to dismiss the indictment. Thereafter on June 23, 2005, the Defendant filed his notice of intention to withdraw the motion to suppress and to file a motion to dismiss the indictment. The undersigned then ordered the motion to dismiss be filed no later than June 29, 2005, and set a hearing on July 7, 2005, in the event the parties wished to address the motion to dismiss on the record. On June 29, 2005, the Defendant filed his motion to dismiss the indictment. Subsequently, on July 7, 2005, the Defendant appeared with counsel on the record and formally withdrew the motion to suppress evidence and statements, and briefly spoke to the motion to dismiss. The undersigned accepted the Defendant's waiver as knowingly made, and indicated that a ruling on the motion to dismiss would be forthcoming.

#45 Defendant's Motion to Dismiss

In his motion to dismiss the indictment, the Defendant claims that the Defendant's use of a computer to allegedly intrude upon a computer which was connected to the internet, does not present sufficient interstate nexus to charge the Defendant with a crime. In essence, the Defendant states that because all of his actions in accessing the protected computer were done in an intrastate manner, his actions were not such that they were used in a "manner that affects interstate or foreign commerce or communications." 18 U.S.C. § 1030(e)(2)(B) supra.

The Defendant is charged with knowingly causing the transmission of a program, information code, or command, and, as a result of such conduct, intentionally causing damage without authorization to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A)(i), in an indictment that, as the government states, tracks the statutory language of this statute. Further, a protected computer as defined by 18 U.S.C. § 1030(e)(2)(B) is defined as a computer "which is used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). Nowhere in the statute is there a requirement that the Defendant's transmission which he communicated to the "protected" computer need to have traveled in interstate commerce. In the case of United States v. Mitra, 405 F.3d 492 (7th Cir. 2005), the Defendant's conduct in sending an attack on a computer system in Wisconsin took place from the state of Wisconsin and was totally contained, at least as far as the attack was concerned, within the state of Wisconsin. The computer itself, however, was found to have been used in interstate commerce. In stating that the nexus of the protected computer is sufficient, the court stated as follows:

> The statute does not ask whether the person who caused the damage acted in interstate commerce; it protects computers (and computerized communications systems) used in such commerce no matter how the harm is inflicted. Once the

> computer is used in interstate commerce, Congress has the power to protect it from a local hammer blow or from a local data packet that sends it haywire.

United States v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005).

In the case at bar, the government contends that it will prove, and the Defendant does not dispute, that the Salvation Army computer attacked by the Defendant was connected through the internet to many entities and individuals outside the state of Missouri. The government has stated that it will prove at trial (and again the Defendant does not dispute), that all of the e-mail communications made by the local Salvation Army on its computer to recipients outside the Salvation Army move from its computer in Missouri to Salvation Army computers in Chicago, and then through Salvation Army computers in London where the Salvation Army's internet portal was located. The government, thus, will prove not only that the computer which was attacked was connected to the internet, but also that this computer was used to communicate in interstate commerce over the internet.

Thus, based on the above case law as well as the plain language of the statute, the undersigned concludes that the indictment alleges and the government will prove a sufficient connection to interstate commerce to allow the indictment to stand. In this case, as stated, the computer was used directly in interstate commerce, and therefore, it meets the test for a protected computer both under United States v. Mitra, supra, and the plain language of the statute. The Defendant's case law which he cites does not stand for the opposite of this proposition.

Therefore, the Defendant's Motion to Dismiss should be denied.

* * *

In accordance with the Memorandum above,

IT IS HEREBY RECOMMENDED that (Doc. #45) Defendant's Motion to Dismiss be **denied**.

Further, the parties are advised that they have eleven (11) days, in which to file written objections to this recommendation and determination. Failure to timely file objections may result in waiver of the right to appeal questions of fact. Thompson v. Nix, 897 F.2d 356, 357 (8th Cir. 1990)

Finally, the parties are hereby notified that the trial of this matter is set on **September 6, 2005, at 9 a.m.**, before the Honorable Rodney W. Sippel, United States District Judge, Courtroom 10-South.

/s/ Terry I. Adelman
UNITED STATES MAGISTRATE JUDGE

Dated this 28th day of July, 2005.